Subject **Prevention Against Cyber Espionage - (Advisory No 17) March, 2018**

1. **Introduction.** A malicious email named as **"List of Authorities"** is being sent to officers and staff of defense/intelligence organizations. The email contains a malware hidden in a **ZIP file** which contains a malicious executable. Downloading and running the file, executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Emails**

   a. **Subjects**. List of Authorities

   b. **Name of Attachments.** 27 Feb2018.zip

   c. **Antivirus Detection Rate.** 14/67 **(20.9% Very Low).**

   d. **Malware Type.** Trojan based Keylogger.

   e. **C&C Servers**

Ser	URL	IP	Hosting Country
a.	http://220.158.216.12 7/search-sys-update-release/base-sync/db7749ID.php	220.158.216.127	Japan
b.	9.147.21.46.in- addr.arpa	46.21.147.9	Netherland

3. **Indicators of Compromise.** The malware makes following files on the infected system:-

   a. C:\Users\<admin>\AppData\Download**27Feb2018.zip**

   b. C\Users\<admin>\AppData\Local\Temp\weatherinfo.exe

4. **Capabilities of Malware**

   a. The malware is capable of getting system IP, user location, network configuration details, computer configurations; and it can upload these details on its C&C server mentioned in para 2e.

   b. The malware has the ability to act as a keylogger and steal he usernames and passwords of infected systems.

   c. The malware can copy itself into registry and it can automatically execute itself on windows boot.

5. **Recommendations.**

   a. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

   b. Block C&C Servers at para 2e in firewalls of own networks.

c. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from intemet and reinstall windows.

d. Update all softwares including Windows OS, Microsoft Office and all other softwares.

e. Don't download attachments from emails unless you are sure about the source.